

BEST AVAILABLE COPY**REMARKS**

Applicant wishes to thank the Examiner for reviewing the present application.

Double Patenting

The Applicant notes the provisional rejection under the doctrine of obviousness-type double patenting in view of co-pending Application No. 09/931,013. However, the '013 application has been abandoned, and thus this objection is moot.

Claim Rejections

The Examiner rejected claims 1-7, and 10-16 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 5,999,626 to Mullin. The Applicant respectfully traverses the rejections as follows.

The present invention is directed towards a method for improving the efficiency of multiplying an elliptic curve point Q with an integer k . In claim 1, the integer k is represented as a set of components k_i , such that $k = \sum_i k_i \lambda_i$, and this representation is used to obtain a value of kQ from $k_0Q + k_1\psi(Q) + \dots$. The value k is selected, that value is represented as a set of components, and those components are added to determine kP . In other words, the method begins with a value of k and computes a scalar multiple of P .

Mullin teaches the application of the Frobenius operator to sets of precomputed points (k_i, k_iP) to compute a pair (k, kP) . Mullin starts with the sets (k_i, k_iP) a priori and ends with the computed point (k, kP) a posteriori. Mullin does not teach how to compute a scalar multiple of a point, but rather teaches how to derive a new point from an existing point, and how to derive the corresponding scalar multiple for the new point.

In the general embodiment of Mullin shown in Figure 3, the starting point is a key pair k_2, k_2P used to derive new values k_n, k_nP . k_nP is obtained by the application of the Frobenius operator to the point k_2P , and there is no contemplation of multiplying k_2P by another scalar k to obtain k_nP . In other words, figure 3 of Mullin does not suggest generating a new k and performing a scalar multiplication on a point. In fact, Mullin teaches independently deriving the new value of k through the use of λ_i , which in turn depends on the number of Frobenius operations performed on the point. However, the value of k computed is the scalar multiple of

BEST AVAILABLE COPY

the seed point P , not the scalar multiple to get from k_2P to k_3P . Mullin therefore teaches computing a value that does not correspond to a scalar multiple, but rather depends on the two points chosen, and cannot be selected by a generator.

The Examiner has referred to various passages in Mullin to support the above rejection. However, none of the passages cited suggest representing a scalar in the way recited in claim 1, and combining it with a point to generate a new point.

Moreover, the embodiment of Figure 4 of Mullin shows the combination of two points, namely k_1P and k_2P , to obtain a third point k_3P . Again, however, there is no scalar multiplication of a point, simply a Frobenius operation and a point addition.

Accordingly, Mullin fails to teach a method of multiplying a point Q by a scalar k , or representing the scalar k in the form required in claim 1. Therefore, claim 1 is believed to clearly and patentably distinguish over Mullin. Claims 2-9 are either directly or indirectly dependent on claim 1, and as such are also believed to distinguish over Mullin.

Claim 10 is directed to a method which also involves generating a new k and performing a scalar multiplication on a point Q , and therefore, the arguments made in respect of claim 1 apply equally to claim 10. Claims 11-18 are directly or indirectly dependent on claim 10, and as such, are also believed to distinguish over Mullin.

The Examiner rejected claims 9 and 18 under 35 U.S.C. 103(a) as being unpatentable over Mullin in view of U.S. Patent No. 6,243,467 to Reiter. The Applicant respectfully traverses the rejections as follows.

In order for there a *prima facie* case of obviousness to be established, Reiter must at least teach, *inter alia*, the elements of the claims not taught by Mullin. The Applicants will show that Reiter does not teach generating a new k and performing a scalar multiplication on a point Q .

Reiter teaches computing kP for a given input integer k by using the Frobenius endomorphism ϕ to write $k = \sum_i k_i \phi^i$. However, Reiter teaches the use of a decomposition algorithm that uses very specific properties of the Frobenius endomorphism. These properties do not hold for an arbitrary endomorphism.

In particular, Reiter teaches decomposing a given integer k as $k = \sum_i k_i \phi^i$ by repeated

Appl. No. 09/885,959

Reply to Office Action of: June 22, 2005

BEST AVAILABLE COPY

division by τ in the ring $Z[\tau]$. The fundamental property is that an arbitrary element γ in $Z[\tau]$ may be written as $\gamma = q\tau + k$ in the ring, where the quotient q and the remainder k are in the ring, and $N(k) < N(\tau)$, where N is a Norm function in the ring. Continuing in this manner by dividing the quotient q by τ often produces a representation of γ as $\sum k_i \tau^i$ in the ring as desired.

Reiter, however, does not teach a method of multiplying a point Q by a scalar k , or representing the scalar k in the form required in claim 1. Therefore, Reiter does not teach the missing elements from Mullin, and as such, claims 1-18 are believed to be patentable over the combination of Mullin and Reiter.

The Examiner has rejected claims 8 and 17 under 35 U.S.C. 103(a) as being unpatentable over Mullin in view of Menzes. The Applicant respectfully traverses the rejections as follows.

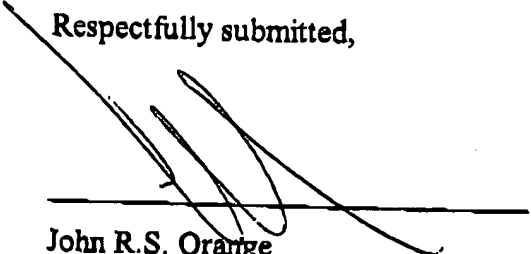
Claims 8 and 17 are ultimately dependent on claims 1 and 10 respectively, and Applicant has shown above that Mullin cannot anticipate claims 1 and 10. Therefore, Menzes must not only teach what is recited in claims 8 and 17, but also what is missing from Mullin.

Menzes does not teach determining kP from the addition of components representing a selected value k as recited in the claims, and as such, claim 8 and 17 are believed to patentably distinguish over Mullin in view of Menzes.

Accordingly, the Applicants believe that claims 1-18 clearly and patentably distinguish over Mullin, and the combinations of Mullin and Reiter and Mullin and Menzes, and as such, are in condition for allowance

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: December 15, 2005